DRAFT

Department of Administration Information Technology Security Policy

Developed by the DofA Security council
October 11, 1999

Security Policy 1

1. Introduction 4

A. General Policy Statement 4

B. Scope 4

C. Compliance 4

D. Document Changes and Feedback 5

E. Security Acknowledgement Form 5

2. Organizational Roles & Responsibilities 5

A. Agency Head 5

B. Data Owners 5

C. Custodians 6

D. Users 6

E. Security Access Administration 6

F. System Administration 7

G. Database Administration 7

3. Computer and Network Operations 7

A. Application System Development 7

4. Vendor/Contractor Relationships 8

5. Security Incident Reporting 8

6. Application & System Security Planning Process for Development or Modification 9

A. Projects which DO NOT Require Department of Administration Resources, Systems or Network Connections 10

B. Projects which Require Department of Administration Resources, Systems, or Network Connections 10

7. Information Security 10

A. Authorized Use and Ownership of Information Resources 11

B. Availability of Critical Data & Systems 11

C. User Accountability: Userids and Passwords 11

D. Access Controls 13

E. Audit Trails 13

1. Security Administration Activities. 13

F. Application Security 14

G. Adapting Policies and Procedures 15

8. Security Implications for System Development and Testing _________________ *15*

9. Authentication, Data Encryption & Key Management _________________ *16*

A. Authentication _________________ **16**

B. Encryption _________________ **17**

C. Encryption Requirements _________________ **17**

D. Encryption Services _________________ **17**

E. Considerations for Data Encryption Systems _________________ **18**

F. Encryption and Authentication Keys _________________ **18**

G. Key Management - Also known as Public Key Infrastructure (PKI) _________________ **19**

H. Data and File Encryption _________________ **20**

10. Network Security Policies _________________ *21*

A. General Network Controls _________________ **21**

B. Distributed Network Access Security _________________ **22**

C. Network connectivity and Monitoring Controls _________________ **23**

D. System Identification Screens _________________ **24**

11. Personal Computers and Agency Equipment Policy _________________ *25*

A. Practices _________________ **25**

12. Physical Security & Asset Security _________________ *28*

A. Access control measures _________________ **28**

B. Fire Suppression Measures _________________ **29**

C. Environmental Measures _________________ **30**

D. Electrical Power Measures _________________ **30**

E. Office Space _________________ **30**

13. Issue-Specific Policies _________________ *31*

A. Internet and E-Mail Access _________________ **31**

B. Voice Communication System _________________ **32**

C. Remote Access _________________ **33**

D. Video _________________ **33**

E. Virus Protection _________________ **34**

14. System Specific Policies _________________ *35*

Appendix A: Security Acknowledgement (need employee orientation training) _____ *36*

Appendix B: Glossary of Terms _________________ *37*

Appendix C: Department of Administration Security Council Members ___________ *41*

1. Introduction

The purpose of the Department of Administration Information Technology Security Policy is to provide security and control policies that comply with Statewide Information Technology Security Policies and apply to all Department of Administration computing and network environments. If there is a conflict between this document and another Department of Administration policy document, the document with the more stringent control takes precedence.

The foundations of this policy are the security concepts of:

- Business need-to-know;
- Least privilege;
- Separation of duties;
- Risk Management;
- Accountability; and
- Auditability.

A. General Policy Statement

Information is a State of Kansas asset requiring protection commensurate with its value. Measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional, as well as to assure its authenticity, integrity, availability, and confidentiality.

B. Scope

The controls in the Department of Administration Information Resource Policy are the minimum requirements for providing a secure environment for developing, implementing, and maintaining systems in the Department of Administration.

This policy applies to all Department of Administration entities, agents, employees, contractors, or vendors involved in the development, implementation, and maintenance of information systems.

Any exception to this policy should be reviewed by the Security Council and receive their documented approval.

C. Compliance

All Department of Administration employees, agents, contractors, and vendors are responsible for understanding and complying with all Department of Administration Information Technology Security Policies. This would include building and configuring systems in accordance with these policies. Non-compliant situations will be brought to the attention of management for appropriate action. Depending on the severity, employees who violate these policies may receive disciplinary action, up to and including immediate dismissal, criminal prosecution, and/or loss of network connectivity.

Outsourced processing and storage facilities, such as service bureaus, vendors, partnerships, and alliances, must be monitored and reviewed to ensure either compliance with Department of Administration policies or that a level of control is provided which is equivalent to Department of Administration policies. This should be accomplished through contractual commitments with provisions to permit auditing and monitoring to ensure compliance.

All necessary exceptions to this policy must be clearly documented and approved by the agency head and the Chief Information Technology Officer for the Executive Branch..

D. Document Changes and Feedback

This document will be reviewed and updated annually. If there is a major change during the year, an addendum will be issued and communicated to managers for dissemination to appropriate personnel. Discrepancies should therefore be reported as soon as possible to the Department of Administration Security Council for review and inclusion in the next version or addendum.

E. Security Acknowledgement Form

Management is responsible for ensuring all employees have a copy of the Department of Administration Information Technology Security Policy and for maintaining **a** signed acknowledgment form from their employees. Employees are responsible for: reading and following policies within this document, signing the security acknowledgement form (found in Appendix A), and returning the signed form to their supervisor/manager. The security acknowledgment forms should be read and signed annually.

2. Organizational Roles & Responsibilities

Information security requires the active support and ongoing participation of individuals from all departments and management levels of the organization. It requires support from the executive level and compliance from everyone.

The following are suggestions for specific roles and responsibilities both at the management and staff level. When roles and responsibilities are assigned, the “separation of duties” concept must be taken into consideration to ensure Department of Administration’s assets are adequately protected.

A. Agency Head

The agency head, with the Chief Information Officer and Division Directors, are ultimately responsible for carrying out the security policy in the Department of Administration and for the development and implementation of the agency security plan.

B. Data Owners

Data owners are the person(s) responsible for collecting, ensuring protection of, and authorizing access to data. For the Department of Administration the owners of data are the Division Directors. Data owners, as senior managers, should assess the risks to the integrity, confidentiality, and availability of information systems data and resources.

The owner is responsible and authorized to:

- approve all access to resources under his or her responsibility;
- judge the asset’s value and label the data as such;

- ensure compliance with applicable controls through regular review of data classification and authorized access.

C. Custodians

Custodians are those person(s) delegated the responsibility of managing, handling or protecting access to data by the Data Owner.

Custodians are responsible for the safety and integrity of data in their custody.

The custodian has responsibility to:

- implement the controls specified by the data owner;
- provide safeguards for information resources;
- administer access to the information resources and make provisions for timely detection, reporting, and analysis of unauthorized attempts to gain access to information resources.

The Executive Branch Chief Information Officer coordinates data owners and custodian responsibilities and serves as the caretaker for security administration.

D. Users

Users are all people who use State information assets for business purposes. This means that the user must protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

Users have the responsibility to:

- use the resource only for the purposes specified by its owner;
- comply with controls established by the owner or public law;
- prevent disclosure of sensitive information.

E. Security Access Administration

The security access administration function provides administration for user access to systems. These responsibilities include, but may not be limited to:

- authentication (add, change, delete) services to provide userids with logonids and passwords;
- authorization (add, change, delete) services to provide user access to applications;
- generation and distribution of reports for monitoring access and potential security breaches. Reporting and monitoring activity should include reports based either on the individual initiating the event or the data and resources affected by the event. These reports should be distributed on a regular basis to the data owners. Reports can include: attempted or actual access violations for data and resources, invalid logon attempts, access trends and deviations from those trends, access to sensitive data and resources, access to data or resources by privileged users, or, access modifications made by security personnel.
- Developing an incident handling procedure.

F. System Administration

The system administration function monitors performance, provides problem determination, production support, and performs system back-ups. Security responsibilities can include, but may not be limited to, ensuring that:

- only authorized software is installed via authorized means;
- approved security procedures are followed and procedures are established where necessary;
- systems are recovered in a secure manner;
- ad hoc system reviews are performed to identify unusual activity;
- systems are installed and operated using no less than the security controls provided by the vendor and using any security controls specified in the Agency's applicable security policies;
- the security access administration function is notified of changes to software that might impact system security features before installation of those changes; and,
- procedures for software license validation and virus testing have been followed.

G. Database Administration

The database administration (DBA) function at Department of Administration has responsibility for other agency owned databases. DBAs are responsible for the development, maintenance, and integrity of these databases unless otherwise specified by the database owner. Security responsibilities include, but may not be limited to:

- designing, developing, organizing, managing, and controlling the database in accordance with security policies;
- providing the security access administration function with the necessary information to maintain user IDs and privileges; and,
- recovering databases in a secure manner when damaged or compromised.

3. Computer and Network Operations

The computer and networks operations and support functions are responsible for operating, supporting, and managing information systems and networks in accordance with the security policies of Department of Administration and those of the agencies whose information they are custodians of. They shall monitor resources for signs of security violations; ensure systems and network architectures maximize security of those resources; coordinate configuration with security administration to ensure all security policies are correctly enforced; ensure network security doesn't conflict with application security; and follow specified escalation procedures for reporting security violations.

A. Application System Development

Application and system developers are responsible for ensuring that the systems he or she develops are created according to the Department of Administration security policies and any additional technical specifications that may apply.

4. Vendor/Contractor Relationships

Allowing access to State of Kansas information to anyone outside the Department of Administration may be necessary at times but this access must be carefully considered. There are occasions when vendors and contractors will require access to State of Kansas systems and the Department of Administration must take precautions to protect all State of Kansas information.

- Access may be restricted to specific terminal locations and granted for a period of days, weeks, or months, and should automatically expire at the end of the period. Access should be restricted to specific IT data or resources.
- It may be appropriate to restrict the contract employee's competitive activities if such activities could take unfair advantage of disclosed information.
- The contract agreement should specify each party's rights on termination of the contract and should specifically address: retention and continued use of the disclosed information by the contract employee, length of time that the nondisclosure requirements remain in effect, return of documents or other materials to the hiring party, liabilities of contract employees, agency, or contract company, and employer..

All vendor/contractor contracts within Department of Administration are handled through the Division of Purchases. Contact the Division of Purchases for more information.

5. Security Incident Reporting

It is the responsibility of all State of Kansas employees to report suspected security violations as quickly as possible. Subsequent action, depending on the type of breach, can vary. The ultimate goal, regardless of the category of incident, is the protection of state assets, containment of damage, and restoration of service. Secondary goals are dependent on the category of violation.

The Security Council is responsible for ensuring procedural documentation exists for handling the various types of security breaches, such as:

- Reviewing and analyzing incident tracking databases
- When appropriate, notifying the workforce of known incidents and precautionary measure Department of Administration employees should be taking.
- At least yearly, reviewing the reporting procedures to insure they adequately address needs

The following considerations apply to reporting procedures for all types of security breaches.

- All employees should immediately report suspected security breaches to their supervisor.
- Supervisors must notify the appropriate business area manager who in turn will notify the DISC Telecommunications manager. The Telecommunications manager will notify the Security Council.

- A detailed report of the security incident should be completed as the details are learned. This report will be filed with the DISC Telecommunications manager who in turn will forward the report to the appropriate Division director and the Secretary of Administration.

- Within 30 days, a follow up report should be completed by the manager of the business area involved describing what actions were taken to remedy the breach.

In addition to the general reporting requirements stated above, the following requirements pertain to specific categories of security breaches.

- For catastrophic disasters such as fire, bomb threats, hostage situations, floods or destructive storms, the secondary goals of employee safety and damage containment apply. Notification procedures will include the appropriate public service departments (Fire Dept, Police Dept, and/or Emergency Management).

- For intrusion of secured areas, the secondary goals of employee safety, intruder identification, intruder's need to be in the secured area, intruders intend and, if warranted removal from the premises apply. Notification procedures will include the Capitol Area Security team and potentially Topeka Police Dept.

- For cases involving electronic intrusion, the secondary goals of data integrity, data recovery, method of breach and intruder identification apply. Notification procedures could include the KBI (if deemed serious enough), the potentially affected business area manager, software application support manager and data center manager. Any activity monitor data, collected as a normal part of doing business, should be kept until the incident has been cleared.

- For cases involving deception and fraud, the secondary goal of identify the perpetrator applies.

6. Application & System Security Planning Process for Development or Modification

A security plan is required for all projects involving development and implementation of new systems or modification to existing systems where there is a change in access or functionality. This includes pilot projects, proofs of concept, temporary access to production systems, and development environments. If an approved security plan already exists and changes are made to the technology used, network, access methods, controls, or classification of data, then an addendum is required. This addendum must be reviewed and signed by the same management levels as the original security plan and provided the same distribution as the original.

All security plans, as well as this document, are confidential and should be shared on a need to know basis. Those who have possession of this document must sign a confidentiality agreement. When employees leave the Department, the immediate supervisor must obtain this security document from the employee and return it to the Chair of the Security Council. The Chair will update a list of employees who have a copy of this document.

The Department of Administration Security Council should be contacted in the beginning phase of all system projects. Projects, which require access to Department of Administration applications or connections to the Department of Administration controlled network(s) must work with the DISC, Bureau of Telecommunications for network design and development of a security plan. The project manager must obtain sign-off by the owner and the Department of Administration Security Council before any network connectivity is established.

The security plan should include, but is not limited to:

- Project Purpose and Overview;
- Architectural Diagram (hardware, software, and network configuration);
- Access Authorization Matrix;
- Data Classification;
- Standards Compliance;
- Standards Exceptions, Risks and Mitigating Controls;
- Change Management procedures;
- Business Continuity Planning;
- Testing Schedule and Target Production Date;
- Sign-off by:
- ▪ Owner
- ▪ Project Manager
- ▪ Department of Administration Security Council

A. Projects which DO NOT Require Department of Administration Resources, Systems or Network Connections

Projects which do not require Department of Administration resources, systems, or connections to Department of Administration controlled networks, do not require review and recommendation by Department of Administration staff. However, they must develop a security plan, which shows all State information is being protected.

B. Projects which Require Department of Administration Resources, Systems, or Network Connections

The Department of Administration Security Council should be contacted in the beginning phase of each project. Projects requiring Department of Administration resources, systems, or network connections must work with the DISC, Bureau of Telecommunications for network design and the Department of Administration Security Council to develop a security plan. The Department of Administration Security Council will review the plan and make recommendations to the Project Manager or author. The Project Manager must then obtain sign-off by the owner and the Department of Administration Security Council Chair (DISC Telecommunications Director) prior to production, and/or before any network connectivity as described above.

7. Information Security

Protecting Department of Administration's information assets is a process, which incorporates many compensating controls. Standard industry information security policies require that agencies identify, classify and protect the automated files, databases and applications that they own. Classifying information and the applications that function to process it is at the heart of identifying and selecting appropriate security and risk management practices. The Department of

Administration's security objectives must include maintaining information integrity and confidentiality while assuring the availability of critical information technology support services.

A. Authorized Use and Ownership of Information Resources

All information and telecommunication resources leased or owned by Department of Administration and all processing services billed to Department of Administration are only to be used to conduct State government business, except as otherwise provided by management directives.

All computer software programs, applications, source code, object code, and documentation is Department of Administration property and will be protected as such if developed either:

- by Department of Administration employees in the course and scope of their employment or with the use of Department of Administration equipment, materials, or other resources; or
- by contract personnel acting under a contract with Department of Administration, unless the contract under which the software or documentation is developed specifically provides otherwise; or
- with Department of Administration funds.

All computer software programs, applications, and documentation purchased for the use of Department of Administration is Department of Administration property and will be protected as such.

It is a violation of Department of Administration policy to copy proprietary software in violation of a licensing agreement.

B. Availability of Critical Data & Systems

The State of Kansas, Executive Branch Chief Information Technology Officer requires agencies to have a Business Continuation Plan that includes the procedures necessary to assure the continuation of vital State operations in the event of a disaster. Each division within Department of Administration must identify and prioritize its processes in it’s continuation plan..

The Business Continuation Plan must outline the internal policies and procedures that are to be employed should a disaster occur. Preparation of the recovery strategies for all time-sensitive processes must be coordinated with Department of Administration’s Business Continuation Manager. In the event of a disaster all time-sensitive services, systems and applications must be restored and available on a priority basis to maintain vital State operation.

Time-sensitive applications include those systems whose loss or unavailability is unacceptable to the citizen’s of Kansas. The loss or unavailability of support services provided to these applications may adversely affect the continuation of vital programs and services or the fiscal or legal integrity of Department of Administration operations.

C. User Accountability: Userids and Passwords

User Ids and passwords will only be issued after receiving a properly authorized request form, indicating type of access desired along with a signed Security Policy statement.

Passwords are pre-stored combinations of characters used by the host computer to authenticate the identity of a individual. Based on the password, the Information Technology system can restrict or grant specific privileges. Passwords are only effective if they remain confidential.

Properly implemented and managed, userids and passwords will improve the likelihood that users are who they purport to be and that a user's access can be controlled effectively. Both are important deterrents to intrusion.

Each user of a multiple-user automated system shall be assigned a unique personal identifier or userid with authorization by the employee's Supervisor. User identification shall be authenticated before the system may grant that user access to automated information.

A user's access authorization will be removed from the system when the user's employment is terminated or the user transfers to a position where access to the system is no longer required. Removal notification is prepared by the immediate supervisor or manager and directed to the Senior Director in each Division. Removal notification must also be provided to the personnel department processing the termination to ensure the termination or transfer is occurring.

Many software and hardware systems come with vendor installed default passwords immediately. If vendors require access to the system remotely for maintenance, they should be provided temporary passwords, that are changed after they have concluded any maintenance.

Passwords must be:

- individually owned;
- kept confidential;
- changed whenever disclosure has occurred or may have occurred, and changed at least every 30 days;
- changed significantly (i.e., not a minor variation of the current password);
- a minimum of six characters and contain alphanumeric characters.
- Encrypted when held in storage or when transmitted over communications networks;
- Suspended (i.e. the userid) after no more than three unsuccessful logon attempts;
- Limited to one use when initially issued or when reset or reissued by security administration personnel.

Passwords must not be:

- shared with other users;
- repeated for at least two cycles of change;
- repeating sequences of letters or numbers;
- names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names);
- the same as the userid;
- stored in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner. The Department of Administration Security Administrator must approve all exceptions;
- displayed during the entry process.

D. Access Controls

Information access control systems are a means of safeguarding the information assets of Department of Administration and the State of Kansas. The following points help identify attributes of an effective information access control system.

- The authority to read, write, modify, update, or delete information from automated files or databases should be established by the owner(s) of the information. Individuals may be granted a specific combination of authorities**.** However, individuals shouldn't be given any authority beyond their needs. For example, an individual may be allowed to "read only" or to "read and write but not delete" data. Specific access authority should be established on a need to know basis.
- Security administration should not require programmer intervention.
- Identification should be unique for each user of the system.
- The system should provide a method to validate the user is who he/she purports to be (e.g., passwords, smart tokens, smart cards).
- Enforcement of strong password controls.
- Authorization to information should be specific as to who is allowed access and what information can be accessed.
- Security administration activity should be recorded and reviewed and security violations should be detected and reported.
- There should not be any access available to Programmers that is not provided through standard, approved connections. In other words, "backdoor" access through dial access devises to a programmer's personal workstation should not be permitted.
- Programmers responsible for development activities should not have access to programs once they have been moved into production.
- Access rules or profiles should be established in a manner that restricts departmental employees from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.
- Procedures are enforced so that application programmers are prohibited from making unauthorized program changes.
- Access for users/application programmers should be limited to specific types of data access (e.g., read, update) required to perform their functional responsibilities.

E. Audit Trails

1. Security Administration Activities.

Audit trails must be maintained to provide accountability for all security administration activity. Software products used to administer security on all Department of Administration systems, such as Top Secret and CA-Unicenter, must be able to record and report all security administration activity. Systems should also provide a means to recover current and historical information about security administration activities in the event of a system failure.

Security administration products and procedures must log all security violations. Resultant log files should be reviewed by security administrators and data owners to detect any unusual or inappropriate activity. In addition to checks against authorizations, particular attention should be paid to unusual times, frequency, and length of accesses, as well as irregularities which could indicate potential violations. Log data must be kept at minimum of 30 days.

The system must not disclose passwords through reporting functions.

Procedures must exist to maintain the integrity of access tables within security enforcement software. The procedures must include “triggers” to insure userids for employees leaving or changing jobs are suspended or deleted. Each Division must assign a person who will be responsible for deleting user IDs.

2. Data Base and Other Logging.

Automated chronological or systematic records of changes to data are important in the reconstruction of previous versions of data in the event of corruption. These records are useful in establishing normal activity, identifying unusual activity, and in the assignment of responsibility for corrupted data.

A complete history of transactions will be maintained for each session involving access to confidential/protected nonpublic information to permit an audit of the system by tracing the activities of individuals through the system. The department’s owner of data must determine how, where, and, the length of time that these transactions will be maintained.

In addition to system start-up and shutdown times, transaction histories should log the following information:

- update transactions;
- date, time of activity;
- user identification;
- sign-on and sign-off activity; and
- confidential/protected nonpublic display transactions.

Only designated personnel should have access to the transaction histories and to the results of any analyses.

3. Data Integrity

Regularly scheduled backups are an integral part of Data Security. The ultimate responsibility for establishing backup procedures lies with the data owner. Backups of mission critical data must be kept offsite to insure recoverability in the event of a natural disaster. Depending on individual circumstances, backups can be any of the following:

- Complete file copies;
- Incremental backup copies which are copies of the changes since the last full backup;
- Database recovery logs which track database activity since the last full backup.

Recovery procedures must be documented and tested on a regular basis. All types of data should be included in backup procedures including but not limited to software program libraries, databases, Job Control libraries and electronic forms of documentation.

F. Application Security

Network access to an application containing private, nonpublic, confidential, or protected nonpublic data, and data sharing between applications, shall be as authorized by the application owners and shall require authentication.

The owner of applications containing non-critical or non-sensitive data should likewise establish criteria for access and user validation, particularly on systems authorized for public use.

G. Adapting Policies and Procedures

Department of Administration programs and supporting computer applications frequently undergo modifications that may affect an existing security system. To ensure that security issues are considered when changes do occur, system documentation should address the impact modifications may have on the existing security system. Security procedures should ensure that the security system and its supporting documentation are periodically reviewed and, if need be, corrective action is planned for and implemented.

8. Security Implications for System Development and Testing

Appropriate Information Security and audit controls must be incorporated into all new systems. Each phase of systems development and testing shall incorporate corresponding assurances of security and audit controls. The ultimate responsibility for insuring appropriate levels of security and audibility lies with the application owner. In conjunction with the application developer, the owner must define the level of security for each phase based on the sensitivity and criticality of the data being processed. The following security aspects will be considered during system development and testing or when new systems are acquired.

1. Determine sensitivity and criticality of the system information. Assess the threats and vulnerabilities that exist relative to the system assets. Perform a risk analysis to quantify potential impact.
2. Identify security alternatives and basic security framework in the selected system architecture
3. Define security requirements and select the appropriate controls
4. Develop security test plans
5. Include approved security requirements and specifications in the development baselines.
6. Conduct tests of security in the configured components and in the integrated system.
7. Prepare documentation of security controls and assign to the documentation the appropriate level of sensitivity.
8. Conduct acceptance test and evaluation of system security.

Change control is a critical security ingredient in systems development, testing and maintenance. To insure security of critical applications, the following change control attributes must be incorporated in all new systems.

1. Only one version of the application programs will ever reside in production libraries
2. The persons writing or maintaining code must not be the same person(s) who migrate code to production libraries

3. The test functions must be kept either physically or logically separated from production functions.
4. Copies of production data shall not be used for testing unless the data has been declassified or unless all personnel involved in testing are otherwise authorized access to the data.
5. Once an application has been placed in production, all program changes must be approved by Application Support Management to insure the changes have been authorized, tested and documented.
6. The software change procedures shall include written notification to the appropriate departments of the change
7. Change control procedures shall be periodically tested by an independent party outside the development function
8. A naming standard should be in effect to distinguish between test jobs and production jobs, test data sets and production data sets.
9. Change Control procedures must ensure that all moves between test and production environments have been authorized in writing by the appropriate manager.
10. Parallel or acceptance tests should be considered production work and therefore run by production personnel.
11. Program development personnel shall access production data and production program files only to resolve emergencies. The manager (or designated supervisor) of Production Control must authorize this emergency access. The appropriate management shall log all such accesses. Procedures must be developed that permit the timely and limited approval of such emergency access as well as the logging and reporting of such access.
12. All programs shall be installed into production from the source code. That is, the appropriate change control staff will recompile the programs into the production libraries.
13. Software generally referred to as “public Domain” software (acquired through software exchanges or electronic bulletin boards) or software not acquired under license or contract shall never be used for processing confidential or sensitive information.
14. Acceptance testing of modified programs should be performed by a quality control function independent of the programming staff utilizing control test files.
15. Only authorized personnel should apply program changes, catalog and copy newly updated programs to production libraries.
16. Automated logs should be used to monitor all access to password tables and production programs. Change Control management is responsible for assuring the logs are reviewed to identify changes in access trends, changes made outside normal business hours, or any other irregular behavior

9. Authentication, Data Encryption & Key Management

A. Authentication

Systems should implement authentication functions that are consistent with the level of confidentiality or sensitivity of the information they contain and process. When considering authentication techniques, first determine if the confidentiality and/or criticality of the information processed by the system requires stronger authentication than passwords alone. If so, the appropriate authentication device should be considered.

Authentication techniques function to protect information by controlling access to the assets of a data processing system. Authentication techniques permit validation of people's identities, hardware devices, and/or transmitted information. Validating or authenticating data and/or the identities of users, terminals, computers, and peripheral devices within a data processing system is vital to the protection of the information the system processes.

Authentication schemes are based on the possession of specific knowledge, capabilities, or personal attributes. They function as challenge-response mechanisms and include password, smart card/token processing, message authentication, and biometric techniques. Having and supplying the correct information authenticates an individual to the data processing system. Similarly, a computer, terminal, or other peripheral may be authenticated as an authorized device of a data processing system. Having and supplying the correct information when it is requested by an authorization system authenticates a device to the system.

Devices -- Several types of authentication devices are available which permit the process of authentication to be inexpensively strengthened. The two most common types of authentication devices are the smart card and the smart token. Both devices strengthen the authentication process by providing its user with a unique computational capability or additional secret information.

The smart card is a passive device that requires a separate reader for operation. The smart token is an active device with keyboard and display. Both devices function in a cooperative challenge/response protocol with system authentication software.

Services -- Authentication services are implemented as specialized secure servers in networks employing the client/server architecture. These servers are used to authenticate clients and their respective servers to each other in a manner that avoids passing readable authentication information across the network.

B. Encryption

Encryption is the process of character substitution or transposition in a sequence determined by an encryption formula. The State of Kansas Statewide Technical Architecture outlines the current & evolving encryption standards. This document should be reviewed before any standard is adopted. Readable text is converted to unreadable text, called cipher text, based on a security key provided by the owner of the information. Anyone examining an encrypted file would see a string of unrelated characters or symbols. The encryption process can be reversed or decrypted only by someone who has the security key.

Data encryption techniques are used to control access to information, protect the integrity of transactions, disguise data during transmission, and authenticate the users and devices of an information processing system.

C. Encryption Requirements

The need for encryption is determined by the classification of the information and the location of the information. Confidential Information which travels over public networks requires encryption.

D. Encryption Services -- The table below contains the security services that may use encryption, a definition of the service, and encryption methodologies currently being used at the Department of Administration.

SECURITY SERVICE	DEFINITION OF SECURITY SERVICE	ENCRYPTION METHODOLOGY USED AT THE STATE OF KANSAS
Confidentiality Protection	Protection from revealing information to unauthorized entities or individuals.	Encryption via VPN (See IT architecture)
Integrity Protection	Preventing data from being modified or manipulated from its original state. In some cases, only integrity protection may be required, then confidentiality protection would not be required.	Checksums VPN
Non-repudiation Protection	The ability to demonstrate to a third party that the originator of a transaction did, in fact, originate that transaction and that the message was not modified.	Digital Certificates

E. Considerations for Data Encryption Systems

The costs associated with a hardware and software data encryption system vary greatly. With respect to the benefits and costs associated with a data encryption system, consider the following:

- What value is attached to the information to be protected?
- Is the information confidential or sensitive?
- What risks are associated with its unauthorized access or undetected modification?
- How long does the information need to be secured (i.e., minutes, hours, days, or years)?
- What are the development, operational, and overhead costs associated with the data encryption system?
- Identify the (1) installation costs, (2) hardware/software costs, (3) personnel training costs, (4) costs associated with changing keys, and (5) system maintenance costs, and (6) additional personnel.
- All encryption algorithms will use a minimum of 128 bit algorithms.

F. Encryption and Authentication Keys

Encryption techniques can be divided into two general categories, symmetric or private key techniques and asymmetric or public key techniques. In private key encryption, the receiver of a message uses the same key to decrypt the message as the sender used to encrypt the message. Public key encryption provides both the sender and receiver with two keys, one private and one public. Private keys are the secret of their users, while public keys are openly available via a directory. When public key encryption is used, the sender encrypts the message in the public key of the intended receiver. Upon reception, the message is decrypted with the receiver's private key. Public key encryption technology simplifies the processes of key distribution and implementation of authentication functions.

G. Key Management - Also known as Public Key Infrastructure (PKI)

The functions associated with generating, distributing, storing, protecting, and destroying authentication and data encryption keys are collectively referred to as key management. Without adopting internal policies and procedures that address key management issues, an agency risks serious security problems. Specifically:

- an unauthorized individual possessing the key and having access to encrypted data might have access to confidential or sensitive information;
- losing the key will render the agency unable to read or process encrypted data; and,
- the agency cannot guarantee the security of its information.

Key management functions should be designed to protect authentication and data encryption keys and associated materials from unauthorized disclosure, substitution, insertion, deletion, and recording. Unauthorized attempts to access key management information should be detectable and unsuccessful.

There are two types of keys that are created and administered by PKI technology.

1. Authentication.

A signing certificate, or key, is provided to a user to be used as a signature attached to documents, e-mail etc. The certificate is provided by the certificate authority (CA).

This is similar to the State of Kansas issuing a Driver's License or ID card to be used as proof of identity. Parties presented with this document have the assurance that the State has collected the information necessary to be certain of the individual's identity.

Similarly, the CA takes the necessary steps to confirm a user's identity before issuing a signed certificate to the user. The user can then attach this certificate to any assurance to the recipient that the information came from the person that signed it. This serves as legal non-repudiation.

The user should protect this certificate since it is his legal signature, if it is in some way compromised this should be reported to the CA administrator immediately so that it can be revoked.

2. **Data encryption keys**.

The CA provides these keys also. Each user is provided with a pair of key, one public and one private.

The private key is used to encrypt data; the public key is used to decrypt it. The public key it provided to anyone the user wished to send information to. This provides security for the data as well as authentication. If the data is intercepted and altered in any way the decryption algorithm will fail.

This encryption may be applied to data in transit over the network and may also be used to protect data stored on magnetic media. Again only the public key of the user can decrypt the data that was encrypted using the user's private key.

The private key should be protected in the same manor as the signing certificate.

H. Data and File Encryption

The Internet is notoriously insecure. Department of Administration employees and contractors should not send any data, classified or not, over the Internet in clear text. This data must be encrypted by approved, strong encryption software.

Properly implemented, an encryption system virtually eliminates risks of disclosure of sensitive information at network nodes and facilities that are not under Department of Administration control, such as the public switched network. Encryption also protects against undetected modification of data and thus enhances integrity as well as confidentiality. Depending on the value of information to an unauthorized recipient, interception or modification of unencrypted information must be recognized as a significant threat.

Security through encryption depends upon both of the following:

- proper use of an approved encryption methodology, and
- only the intended recipients holding the encryption key-variable (key) for that data set or transmission.

1. GUIDELINES FOR DATA AND FILE ENCRYPTION:

In making the determination to use data and file encryption, the following risks should be considered:

- loss of State funds;
- violation of individual expectations of privacy;
- violation of state or federal law;
- civil liability on the part of Department of Administration;
- compromise of Department of Administration legal or investigative efforts;
- loss of business opportunities for affected persons; and
- undue advantage to any person in Department of Administration competitive business relations.

2. Interception of unencrypted information may not be readily detectable. It should be assumed that unencrypted information is available to any intruder.

3. When encrypted data is transferred between organizations, the respective Information Resource Managers should devise a mutually agreeable procedure for secure key management. In the case of conflict, the data owner should establish the criteria.

4. Keys should be communicated separately from the encrypted information, preferably through different channels.

5. Passwords and dial-up terminal identifiers should be encrypted during transmission and in storage. They should be encrypted during session logon if the information to be exchanged requires encryption.

6. Encryption and decryption devices should be located as near the using devices (connected terminals and processors) as possible to minimize the need for other safeguards on the unencrypted segments of the link.

7. Sensitive or critical information should be stored in encrypted form if physical controls are not sufficient. Volumes or files where all sensitive information is encrypted may be controlled as though the information is not sensitive as long as encryption keys are appropriately controlled.

8. Security through encryption may be enhanced by requiring that two trusted individuals control the key; each having custody of half the key.

10. Network Security Policies

There are two types of access: trusted and untrusted. Trusted access refers to access between Department of Administration controlled nodes, systems, or networks. Untrusted access refers to access between non-Department of Administration controlled nodes, systems, or networks and Department of Administration controlled nodes, systems, or networks.

In addition to the types of access, there needs to be considerations for public vs. private networks. Public networks are defined as those accessible to the general public, such as: the Internet, telephone lines, satellite links and wireless or cellular communications. Public networks are considered untrusted therefore, all restrictions as applied to untrusted will be applied to public. Private networks are defined as networks not available to the general public such as any Department of Administration Local or Wide Area Network. Private networks may only be considered trusted if the network is controlled from end to end by the Department of Administration.

A. General Network Controls

Network resources participating in the access of confidential/protected nonpublic information shall assume the confidentiality level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.

All network components under Department of Administration control must be identifiable and restricted to their intended use. Following are some guidelines:

1. Password protected screen savers, terminal lock and key, or terminal software locking options will be enabled on each terminal so that access can be controlled by locking the terminal while it is unattended.

2. All line junction points (cable and line facilities) should be located in secure areas or under lock and key

.

3. Control units, concentrators, multiplexers switches, hubs and front-end processors will be protected from unauthorized physical access.

4. Procedures will be implemented which ensure that access to data or information is not dependent on any individual. There should be more than one person with authorized access.

5. Some types of network protocol analyzers and test equipment are capable of monitoring (and some, of altering) data passed over the network. Use of such equipment will be tightly controlled since it can emulate terminals, monitor and modify sensitive information, or contaminate both encrypted and unencrypted data.

6. DISC is responsible to maintain up-to-date diagrams showing all major network components, to maintain an inventory of all network connections, and ensure that all unneeded connections are disabled.

7. Default passwords on network hardware such as routers should be changed immediately after the hardware is installed.

8. Each Division must maintain a list of all approved dial access modems. Each Division should establish a procedure that periodically checks for any unapproved modems that have been added to the network.

9. Each Division must periodically monitor sharing and trusting relationships to ensure they are still valid

10. One person in each Division should be assigned the responsibility of (1) monitoring security updates that apply to the Division's software, and (2) keeping security patches current.

11. An Audit of network security should be conducted annually.

12. Require an audit of network security before allowing new E-business or Electronic Data Interchange (EDI) applications to go into operation, especially if they involve transfer of funds or the bypass of established security controls.

13. Procedures must be implemented which ensure that access to data or information is not dependent on any one individual.

B. Distributed Network Access Security

Department of Administration owned or leased network facilities and host systems are Department of Administration assets. Their use should be restricted to authorized users and purposes. Where public users are authorized access to networks or host systems, these public users must be clearly identifiable and restricted to only services approved for public functions. Department of Administration employees who have not been assigned a userid and means of authenticating their identity to the system are not distinguishable from public users and should not be afforded broader access.

Owners of distributed information resources served by distributed networks shall prescribe sufficient controls to ensure that access to those resources is restricted to authorized users and uses only. These controls shall selectively limit services based on:

- user identification and authentication (e.g., password, smart card/token); or,
- designation of other users, including the public where authorized (e.g., vendor access through dial-up or public switched networks), for the duration of a session; or,
- physical access controls.

Guidelines for distributed network access:

1. For distributed processing systems and local area networks, authorization at network entry shall be made on the basis of valid user identification (e.g., userid) and authentication (e.g., password, smart card/token).

2. The host security management program shall maintain current user application activity authorizations through which each request must pass before a connection is made or a session is initiated.

3. Unauthorized attempts (successful or otherwise) to access or modify data through a communication network should be promptly investigated.

4. If unauthorized access or modification of data occurs, the Department should promptly review its existing security system, including its internal policies and procedures. Appropriate corrective actions should be planned for, established, and reviewed by the Security Council to minimize or eliminate the possibility of reoccurrence. Employees may need to be reminded of existing or revised procedures.

C. Network connectivity and Monitoring Controls

	CONTROL NAME	CONTROL STANDARD
1.	Connections	No communication modem, router, gateway or other network device or software may be connected to a Department of Administration KAN-WIN network without approval from the DISC, Bureau of Telecommunications. All communications design architectures, connecting to the Department of Administration network, must also be reviewed and approved by the DISC, Bureau of Telecommunications.
2.	Addressing	Network names and addresses should be coordinated by DISC, BOCS.
3.	System and Node Authentication	Each system and node in a network must authenticate each accessing user, process, or other entity. This may be either through individual logon or by means of a single sign-on to a strongly authenticated Department of Administration controlled security server. Connection paths, terminal addresses, node addresses or other identifiers do not constitute an acceptable means of user authentication.

4.	Trusted Node Authentication	The use of trusted nodes requires that the owners of all participating nodes agree to the adequacy of the controls for authentication of users of those nodes. Participating nodes must also authenticate the identities of other nodes. Connection paths, terminal addresses, node addresses or other node identifiers do not, by themselves, constitute an acceptable means of node authentication. Only Department of Administration owned, operated, and controlled nodes located in restricted facilities may be trusted nodes.
5.	Network Diagnostic and Monitoring Tools	Possession, distribution or use of network diagnostic, monitoring, and scanning tools such as LAN analyzer and attack scanners (both hardware and software) is limited to designated and authorized personnel in accordance with their job responsibilities. This includes anything that can replicate the functions of such tools. Unauthorized possession, use, or distribution of such tools or functions is prohibited and may be grounds for immediate dismissal. Attach scanners should not be used outside the Department of Administration unless prior notice and authorization is granted in writing by the targeted agency.
6.	IP Address Classification	IP addresses for firewalls and other security servers are classified as protected nonpublic, therefore, the appropriate classification guidelines should be followed.

D. System Identification Screens

State of Kansas system identification screens may include the following warning statements:

- Unauthorized Use is Prohibited;
- Usage May be Subject to Security Testing and Monitoring; and
- Abuse is subject to criminal prosecution.

Guidelines for system identification screens:

1. The system identification screen should be implemented so that it cannot be bypassed by a user.

2. The system identification screen should remain on display for a sufficient amount of time for the message to be read.

3. If the system cannot display an identification screen with an appropriate warning message, the message should be included on a printed label affixed to each video display terminal.

4. Identification screens for Department of Administration must be approved by DofA Legal.

11. Personal Computers and Agency Equipment Policy

Information is an important agency asset requiring appropriate protection. Measures must be taken to protect information from unauthorized modification, destruction or disclosure, whether accidental or intentional, as well as to assure its security, integrity, availability, and confidentiality.

No Personal Computers should be used for access to Department of Administration resources unless they are specifically authorized by the Division Director. All equipment used for access to DofA resources shall belong to the State, not to the individual employee. This equipment, along with any communications equipment and circuits should be maintained and used under the same guidelines as equipment located in a work environment. The uses of this equipment are responsible for assuring that no unauthorized access is permitted with this equipment.

Inappropriate use of Department of Administration's computer equipment may subject the employee to disciplinary action up to and including termination of employment.

A. Practices

1. Information Security

To be consistent with Information Security industry best practices all information should be identified and protected according to its level of confidentiality and business "need-to-know." Know the level of sensitivity of the information that you are responsible for and with which you work. Information can be group in several categories. Those categories are:

Data on Individuals:

- Public – any information that can be disclosed to anyone for any reason without violating an individual's right to privacy;
- Private – information on an individual that can be disclosed to the individual, anyone authorized by the individual, or by law;
- Confidential – information intended solely for use within Department of Administration and limited to those with business need-to-know.

Data Not on Individuals:

- Public – data that can be disclosed to anyone for any reason without violating an individual's right to privacy;
- Nonpublic – data available only to the data subject and anyone authorized by the data subject or by law;
- Protected Nonpublic – information intended solely for use within Department of Administration and limited to those with business need-to-know.

Do not disclose information which is classified as nonpublic to unauthorized persons. Always verify the identity and the need-to-know of anyone requesting this information. Notify your management of unauthorized attempts to obtain information.

2. Visual Displays:

To prevent someone from viewing information without your knowledge, take precautions such as:

- using a password protected screen saver on your computer monitor;
- erasing white boards containing Confidential or Protected Nonpublic information; and
- immediately remove Confidential or Protected Nonpublic information from printers or facsimile machines; and
- remove and secure Protected Nonpublic information from your desktop.

3. **Wireless Transmissions**:

Do not discuss or transmit Confidential or Protected Nonpublic information on unencrypted cordless telephones, cellular phones or wireless modems because conversations can be easily intercepted and monitored. Never discuss or transmit Confidential or Protected Nonpublic information without explicit authorization.

4. **Computer and Network Security**

Take the following precautions to prevent unauthorized individuals from gaining access to Department of Administration information and systems:

- protect your personal authenticators (passwords, PINs, smart cards, tokens, etc.) so they cannot be used by others;
- do not disclose or share passwords with anyone, including your management;
- do not leave your workstation unattended while logged on without some type of access control (i.e., password protected screen saver); and
- notify your management if you detect any unauthorized use or attempted misuse of your personal authenticators, terminal sessions or equipment.
- Do not write your passwords on paper unless the paper file is secured.
- Do not answer any questions about the network, or how to access data on the network without knowing the person asking the questions. Answers to questions about the network and it's interworking shall only be provided on a need to know basis.

5. **Anti-virus Software**:

All PC’s, servers, and midrange machines must use virus detection and eradication software to scan for viruses. Anti-virus software should be updated frequently. Scanning should be performed:

- during system start-up;
- when a disk is inserted;
- after software installation; and
- before loading programs obtained from external sources (for example, the Internet, vendors or bulletin boards).

Additionally, auto protect features should be enabled to scan a file when it is opened, saved or executed.

6. Data backup and Storage:

Routinely make duplicate copies of information. Store original software programs and backup data copies in a secure place.

7. Portable Computers:

Do not leave portable computers unattended; lock them up when they are not in use. In addition:

- portable computers containing Private or Nonpublic information should use software access controls and anti-theft devices; and
- portable computers containing Confidential or Protected Nonpublic information should use encryption software.

8. Remote Access:

Dial-in access to Department of Administration should be established through the KANSAN dial-up network.

Direct dial-in to modems on Department of Administration (DofA) LANs is not allowed without explicit approval from the DofA Security Officer. The use of software that permits a user to access DofA resources from home or when traveling away from the office should be managed closely to avoid compromising security policies. The use of software similar to PC Anywhere, or Carbon Copy, that make it easy for remote access terminals to function exactly as they would in the office should be avoided. It is the responsibility of the agency Director to assure that this type of software is not used without the proper review and management.

Servers (except email post offices) requiring access from other than authorized DofA personnel shall not be allowed behind the DofA security boundary (firewall or firewall router). Such devices must be located either on the supplied DMZ or on one of the public access LANs such as the datacenter LAN or the Class C external network.

9. Diagnostic and Monitoring Tools:

Distribution or use of network diagnostic, monitoring, scanning tools or hardware/software attack scanners is limited to designated and authorized personnel. If you distribute or use these tools without authorization, it can result in your immediate termination.

10. External Systems

If you have access to the Internet or any other external systems, be sure to follow all appropriate information security policies. For example:

- do not transmit information belonging to Department of Administration outside the agency without appropriate approvals and precautions;

- remember that e-mail and data sent to or received from external systems, such as the Internet, are not secure or private and are easily read; and
- never download and start any programs until you have verified they are not contaminated with a virus.

11. Software and Licensing

Only Department of Administration-approved software should be used. All software must be owned by Department of Administration or properly licensed to Department of Administration by the owner of the software.

12. Privacy

Files and messages you send or receive using agency computing resources and equipment are not private communications. If necessary for job-related reasons, authorized Department of Administration personnel may inspect and monitor the use of computing resources and equipment at any time. The Department does not regularly monitor such communications, but reserves the right to do so.

13. Security Incident Reporting

If a computer is stolen, or if agency information is modified, destroyed or taken in an unauthorized action, notify your manager immediately.

14. De-installing Equipment

When computer equipment is de-installed and staged for surplus property, the DISC CSC must be notified. CSC will purge the machine . Divisions are responsible for removing the device from the inventory records.

12. Physical Security & Asset Security

Physical Security should consider identification of sensative areas, identification of entry and exit points, access authorization (procedures and monitoring devices, alarms), assessment of nearby businesses, natural disaster-prone areas, electrical supplies, manmade threats, specific information system environmental controls, etc.

The following practices must be adopted in order to maintain adequate Physical Security within the agency or Division offices

A. Access control measures:

1. All servers and other sensitive pieces of hardware should be kept in locked rooms.

2. Wiring closets should be kept locked at all times.

3. Secure Storage for laptop computers should be available within all Dept of Administration offices

4. Laptop computers that are used outside the office and that contain confidential information should have some means of protecting the data, such as encryption or maintaining the data on removable disks.

5. All DISC operated computer rooms and Telecommunication distribution frames located throughout the Capitol Complex must be located in rooms with card key access. In addition, access control measures for raised floor computer rooms must include the following.

a. Persons working in DISC computer rooms must complete a level 1 security clearance as a condition of employment.

b. Walls separating work areas on raised floor where the level of security is different on either side of the partition must extend and completely shut off the area between the raised floor and the permanent floor.

c. Only persons whose work requires them to be in raised floor computer rooms on a day to day basis will be granted access cards to those areas.

d. All visitors to computer room facilities must sign in at the Production Control window.

e. Logs of all visitors to computer rooms will be maintained for a minimum of 1 year (????) for audit purposes.

f. The Bureau of Administrative Services (BAS) within DISC is responsible for creating and maintaining procedures for the issuance and removal of card keys.

g. The Data Center Manager is responsible for processing requests for new cards, changes to existing cards and deletions of card.

6. Whenever an employee leaves DISC for other employment the immediate supervisor must obtain building passes and DISC access card keys. The supervisor must also notify the Data Center Manager immediately upon an employee’s separation.

7. All Department of Administration Divisions must have policies and procedures in place for locking doors after work hours. All hub rooms, communications rooms for telecommunications and wiring closets must be secured with key locks, card keys or punch down locks.

B. Fire Suppression Measures

1. All Department of Administration work areas must have hand held fire extinguishers available in accordance with published fire prevention standards for public access buildings. These extinguishers must be checked by a licensed extinguisher inspector on at least a yearly basis.

2. Care must be taken to properly store flammable solutions or materials

3. Fire doors are not to be propped open for any reason.

4. All Dept. of Administration employees will participate in regularly schedule evacuation drills.

5. With regards to Raised Floor Computer Rooms:

a. Low Flame spread materials are to be used whereever practical in the construction of computer rooms

b. Dampers and Shutters are to be included in the heating and cooling subsystems of building housing computers that can be closed to slow the spread of fire.

c. Detection equipment must be included in the construction of computer rooms that activate alarms at a centrally located console area. This equipment must be tested on a regular basis.

d. Sprinkler systems in computer rooms must be of the “dry line” type to prevent accidental discharge of water on electronic equipment.

e. If dry chemical type extinguishing systems, such as Halon, are used in computer rooms, these systems are to be checked by qualified technicians on at least a yearly basis.

C. Environmental Measures.

1. With regards to Raised Floor Computer Rooms.

a. Adequate air handling equipment must be installed to insure room temperatures consistent with computer equipment needs. Redundancy should be included in this plan to accommodate times when primary equipment is down.

b. The area below the raised floor must be thoroughly cleaned at least on a yearly basis to prevent circulation of harmful dust particles.

c. Monitoring equipment must be installed to track temperature and humidity. This equipment must be capable of sounding an alarm should one of these environmental conditions exceed predetermined thresholds.

D. Electrical Power Measures

1. Uninterrupted Power Supply (UPS) systems must be utilized to assure continuous power to systems deemed critical to State of Kansas business.

2. Surge protection equipment should be utilized to protect electronic equipment that might be sensitive to power fluctuations.

3. Anyone working on or around electronic data processing equipment must wear static electricity eliminating bracelets.

E. Office space

1. All Department of Administration Divisions must have policies and procedures in place for locking doors after work hours.

2. All hub rooms, communications rooms for telecommunications and wiring closets must be secured with key locks, card keys, or punch down locks.

13. Issue-Specific Policies

A. Internet and E-Mail Access

1. Security

Access to and from the Internet and through the e-mail system represents potentially significant security exposures for the Department of Administration and the State of Kansas network. The following are the minimum controls required to establish an Internet or e-mail connection using Department of Administration computing or networking resources. It applies to all individuals who use the Internet and/or e-mail with Department of Administration resources as well as those who represent Department of Administration.

Users of Department of Administration systems may not use State of Kansas facilities and connections to make unauthorized connections to, break in to, or adversely affect the performance of other computer systems on the network. Access to other computer systems via the Internet does not convey the right to use or connect to these computer systems. This right only comes from proper authorization by the owners of those computer systems. Individuals must not “test the doors” or “probe” security mechanisms at either Department of Administration or other Internet sites unless they have first obtained permission from the Department of Administration Security Council.

Users of Department of Administration systems are required to use all available methods to prevent unauthorized connections to State of Kansas networks. This includes taking such precautions as enabling approved virus protection software when connected to the Internet or receiving e-mails. This also includes prohibiting unauthorized persons from accessing State of Kansas systems through the user’s logon or password, using password protected screen savers when the work area is unsupervised and taking any other prudent security precautions.

Department of Administration private, nonpublic, confidential, or protected nonpublic information must not be sent over the Internet or through e-mail unless it has first been encrypted by a Department of Administration approved encryption method.

If a user suspects that sensitive Department of Administration information has been lost or intercepted by unauthorized parties, the user is required to notify the Department of Administration Security Council immediately.

2. Privacy

Department of Administration maintains an electronic-mail (e-mail) system and Internet access to conduct State of Kansas business. This system, including the equipment and the data stored on the equipment, is at all times, the property of the State of Kansas.

Department of Administration cannot guarantee the privacy of electronic communications because electronic communications are not private by nature, and are inherently insecure. Employees should have no expectation of privacy when using e-mail systems or the Internet.

Even though passwords appear to provide confidentiality, privacy of messages cannot be assumed. This means that e-mail and Internet transmissions can be read, altered, or deleted by unknown parties without the knowledge or permission of the user who composed, sent, or received the message or its attachments(s). In addition, note that even when e-mail messages or Internet files are deleted or erased, it is still possible to recreate the original message or file.

3. Guidelines on Employee Use

Like all communications conducted on behalf of the State of Kansas, employees must use good judgement in Internet and e-mail use. Each use of the Internet and each e-mail must be able to withstand public scrutiny without embarrassment to Department of Administration or the State of Kansas.

Users are responsible for any and all activity initiated by their e-mail ID, userid or personal workstation.

Individuals must not disclose internal Department of Administration information via the Internet or e-mail system that in any way adversely affects Department of Administration customer relations or public image.

The following log-in warning is displayed on all Department of Administration personal computers:

“WARNING: This technology is provided for official state business only. Inappropriate use (including, but not limited to the e-mail system and the Internet), may result in monitoring. Inappropriate use may result in the proposal of disciplinary action up to and including termination of employment in accordance with K.S.A. 75-2949e(a)(3) and other appropriate statutes. System-wide checks will be conducted on a periodic basis to assure that pornographic sites are not being utilized. Internet/e-mail activity of this highly inappropriate nature that is substantiated will result in the proposal of termination of employment. “

B. Voice Communication System

The Department of Administration telephone system uses Centrex for local and internal communications. Long Distance telephone services is provided by competitively bid state contract. Centrex switches telephone calls to the long distance provider based on standard routing tables. Both services are managed and maintained by DISC.

1. Voice Mail

Voice mail service is provided by a separate processor, managed and maintained by DISC.

Voice mail may be used to receive and retrieve messages when employees are unable to answer their telephone. This service is connected to

Centrex through call routing via extensions and the potential for unauthorized message receiving or fraudulent calling can occur.

The voice mail system provides security protection through the use of user passwords.

The following steps should be taken to minimize fraudulent use of voice mail.

1. Never use easy or obvious passwords and change them often. – The voice mail system age passwords after 30 days and users will be forced to assign a new password.

2. Unassigned mailboxes should be deleted. This is done with a Telecommunications Service Request (TSR) to DISC.

3. Monitor activity logs for repeated login attempts to specific mailboxes or to repeated random login attempts. – This is done by DISC as part of standard management of the system.

4. Lock the mailbox after 3 unsuccessful login attempts.

5. Require users to create personal greetings and to change the default password when setting up their mailbox.

6. When an employee leaves the Department for another employer or agency, the immediate supervisor must notify the voice mail administrator in DISC in order for the administrator to remove the departing employee from the voice mail system.

C. Remote Access

Dial-up access via a modem poses a high risk of possible intrusion to the Department of Administration network. At the same time remote access conveniently enables Department of Administration employees, contractors and vendors to access Department of Administration computer resources from offsite locations.

Department of Administration networked systems should not be accessed over the Internet using Department of Administration assigned logonids unless passwords are encrypted. Other protected transmission means such as the dial-up facilities must be used instead.

D. Video

Video conferencing capabilities are offered to the entire State through the Kansan network. This service is being used for Telemedicine, classroom training, meetings, and public hearings as well as confidential hearings. Following are requirements for video conferencing:

- Video conferencing is done through dedicated T-1 lines.
- Point-to-point and multipoint video connections are made through Department of Administration's Network control Center (NCC).
- No unauthorized recordings will be made of any video conferences.

- There will be no unauthorized play back of authorized conference recordings.
- Operations center employees responsible for administering connections for video conferencing will not record, play back or listen in on conference calls unless they are instructed to do so by the hosting party of the video conference.

E. Virus Protection

Computers infected with viruses or malicious code could jeopardize information security by contaminating data. This policy provides controls to protect against such attacks. Please refer to Information Security Incident Reporting, for appropriate action for detected or suspected viruses.

A typical virus is a small computer program that, as part of its operations, reproduces itself by making copies of itself and inserting these copies into uninfected programs or data files. This insertion process takes only a fraction of a second, a virtually undetectable delay. The infected program will subsequently execute the virus code during its normal processing. In addition to its ability to reproduce, the virus may cause damage to the programs, data, or equipment, or it may perform some other function that is relatively harmless. Viruses can use one or more techniques to achieve their purpose. They can be spread by sharing data files. Personal computing environments are more susceptible to viruses, however, they can occur in the mainframe computing environment as well. The following are controls that can reduce the chance of virus infection within the personal computing environment.

	CONTROL NAME	CONTROL STANDARD
1.	Virus Detection Software	Virus detection or integrity checking software should be used in all PC/LAN environments, including portable PCs and PCs located at employees’ homes.
2.	Updating Virus Detection Software	The data files used by the detection software must be updated at least once weekly to ensure system scans can identify most known viruses.
3.	Loading Software	a) No unapproved software may be loaded on Department of Administration PCs or LANs. b) All software introduced into Department of Administration PC/LAN computing environments, including Department of Administration PCs that are located in employees' homes, must be known to be virus free. c) All PC/LAN computing environments into which Department of Administration software and/or data is introduced must be known to be virus free. d) Software distributed from any Department of Administration PC/LAN computing environment to another Department of Administration organization or an Department of Administration customer must be known to be virus free.

4.	Verifying software	Virus scans or integrity checks must be done prior to the first use of each executable file that is brought into the Department of Administration environment from untrusted environments, e.g. program fixes copied from vendors' bulletin boards or web sites.
5.	Scanning Removable Media	Virus scans or integrity checks must be done prior to the first use of each diskette (or other removable media) after the diskette has been out of an Department of Administration-controlled environment. Examples: Diskettes used in a PC at home, whether owned by Department of Administration or not. Diskettes used in a customer or vendor's computer.
6.	Scanning Frequency	Virus scans of permanent media must be done at least daily: a) On any server connected to a network, e.g. a server connected to a LAN. b) On computers used for distribution of files outside of , e.g. those used to send files to external customers, user groups, or vendors c) On any workstation that shares software with any other computer. d) On computers running an application for which the risk is medium or high for loss of data or loss of the application. Virus scans must be done at least weekly in all other situations.
7.	Scheduling Virus Scans	Whenever possible virus scans should be scheduled to occur automatically. (All files should be scanned before being loaded on the network and a weekly network scan should be scheduled as well.)
8.	Audit Records	Records must be kept that show scans occurred and the details of any findings from the scans. Note: Some scanning software provides customized logs.

14. System Specific Policies

Each computing platform or device has specific controls which should be maintained. This information should be found in a system specific policy and procedure document. Please refer to this documentation for additional information on security policies and procedures you may need to follow (ex. mainframe, Unix, Windows NT, Novell, firewall). Copies of these policies, procedures, and standards appear in appendix D.

Appendix A: Security Acknowledgement **(need employee orientation training)**

Employee Agreement to Comply with the Department of Administration Information Technology Security Policies

Although the Department of Administration has specialists devoted to information security, it is the responsibility of users to comply with all information security policies and procedures. When the undersigned requests a userid on any Department of Administration automated information system, he/she acknowledges that he/she is a “user” as defined in the Department of Administration Information Technology Security Policy manual. As a user, the undersigned additionally acknowledges that he/she must comply with the security measures dictated by both “owners” and “custodians,” as defined in the Department of Administration Information Technology Security Policy.

As a user, the undersigned acknowledges that he/she is a Department of Administration employee in possession of Department of Administration information resources. This means that the undersigned must protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

The undersigned has read the Department of Administration Information Technology Security Policy and understands the policies and procedures described therein. The undersigned agrees to abide by the policies described therein as a condition of continued employment. The undersigned furthermore understands that violators of these policies are subject to disciplinary measures including privilege revocation and/or employment termination. The undersigned understands that access to Department of Administration information systems is a privilege that may be changed or revoked at the sole discretion of Department of Administration management, and which automatically terminates upon departure from Department of Administration.

The undersigned certifies that he/she has received a copy of the Department of Administration Information Technology Security Policy for future reference.

The undersigned also agrees to promptly report all violations or suspected violations of information Technology security policies to the Department of Administration Security Council.

____
Users signature, today’s date, and location when signing

____
User’s name in block capital letters

____
Witness signature and date

Appendix B: Glossary of Terms

Access: To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

Access control: The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Access password: A password used to authorize access to data and distributed to all those who are authorized similar access.

Account: A set of privileges for authorization to system access, which are associated with a userid.

Authentication: Verifying that a user is who he or she purports to be.

Authorization: The process of granting privileges to an authenticated user or entity.

Algorithm: A mathematical process for performing a certain calculation; in the information security field, generally used to describe an encryption process.

Brute force attack: An attack against an encryption algorithm where the attacker attempts to recover the secret key by trying all possible values. Longer keys are more resistant to brute force attacks.

Business need-to-know: A security concept which limits access only to information and information processing resources required to perform one's normal business related duties.

Business resumption: The ability to resume business after an outage. This is critical to our ability to service our customers.

Challenge/Response Password: A one-time password generating device, token, or SmartCard used in place of a reusable password.

Change management: Change management is documented procedures used to control the revision of applications and or operating systems in computing environments. These controls should involve a separate group (not the original programs) to control the changes to application and/or OS code.

Compliance statement: A document used to obtain a promise from a computer user that the user will abide by system policies and procedures.

Confidential information: A classification for information, the disclosure of which may damage the State of Kansas, Department of Administration, citizens of Kansas, or other involved parties.

Control Statement: A statement that applies to information which informs the user of special requirements, restrictions or protection.

Critical information: Any information essential to Department of Administration's activities, the destruction, modification, or unavailability of which would cause serious disruption to Department of Administration's mission.

Cryptography: The use of an algorithm to encrypt and/or decrypt.

Custodian: Guardian or caretaker; the holder of data; the agent charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource.

Data: A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

Data integrity: The state that exists when computerized information is predictably related to its source and has been subjected to only those processes which have been authorized by the appropriate personnel.

Data security or computer security: Those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction.

Decryption: The mathematical process by which an encrypted message is rendered readable or usable (reverses the encryption process).

Dial-in: The capability to allow one system to access information or receive a message from another system over non-dedicated public phone lines.

Dial-out: The capability to access information on another system and send a message. Dial-out occurs on the system that initiates the call.

Digital signature: A sequence of bits which accompanies a message that is generated via encryption; such a bit sequence shows that a message (a) was sent by an identified person, and (b) is free from modification or tampering.

Disaster: A condition in which an information resource is unavailable, as a result of a natural or manmade occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Disclosure: Unauthorized access to confidential or sensitive information.

Dynamic password: A password which changes each time a user logs-into a computer system (typically accomplished via smart cards).

Encryption: The process of transforming readable text into unreadable text (ciphertext) for the purpose of security or privacy.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

End-user: A user who employs computers to support NAI activities, who is acting as the source or destination of information flowing through a computer system.

Exposure: The condition of vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information resources.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed some security test (such as providing a dynamic password).

Host Computer: Computer that provides a service or application that users access through a network connection. Historically the term has been used to refer to large mainframe computers.

In this document the term includes computers of any size and servers in client-server environments.

Information: That which is extracted from a compilation of data in response to a specific need.

Information resources: The procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Isolated computer: A computer which is not connected to a network or any other computer; a stand-alone personal computer is an example.

Loginid: A character string that uniquely identifies a user on a computer system. This term is mainly used by NetWare.

Log-in script: A set of stored commands which can log a user into a computer automatically.

LogonID: A character string that uniquely identifies a user on a computer system. This term is mainly used in reference to a mainframe.

Network penetration: The attempt or successful act of bypassing the security mechanisms of a system.

Owner: The agent responsible for specific agency resources.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password-based access control: Software which relies on passwords as the primary mechanism to control system privileges and logging activities.

Password: Any secret string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user-ID: A userid which has been granted the ability to perform special activities, such as shut down an application or system.

Production application: A tested, documented, and periodically-executed computer program which performs one or more regular business activities related to Department of Administration's mission; examples include accounts payable and payroll.

Retention schedule: A management-approved listing of the types of information that must be retained for archival purposes and the time frames that these types of information must be kept.

Risk: The likelihood or probability that a loss of information resources or breach of security will occur.

Risk analysis: An evaluation of system assets and their vulnerabilities to threats. Risk analysis estimates potential losses that may result from threats.

Risk management: Decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Router: A device that interconnects networks; used in some instances to provide access control and message routing services.

Security administrator: The person charged with monitoring and implementing security controls and procedures for a system.

Security controls: Hardware, programs, procedures, policies, and physical safeguards, which are put in place to assure the integrity and protection of information and the means of processing it.

Security incident or breach: An event which results in unauthorized access, loss, disclosure, modification or destruction of information resources whether accidental or deliberate.

Security standard: A required procedure or management control.

Sensitive information: Any information, the disclosure of which could damage NAI, business partners, customers, or other third parties.

Separation of duties: No one individual or function has control of entire process. When properly implemented, separation of duties provides the necessary checks and balances to mitigate against fraud, errors, and omissions.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Strong, two-factor authentication: An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. The processes may employ cryptographic techniques in combination with repeated information such as reusable passwords. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

System administrator: A designated individual who has special privileges to maintain the operation of a computer application or system.

System control data: Data files such as programs, password files, security tables, authorization tables, etc., which if not adequately protected, could permit unauthorized access to information resources.

Userids: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Virus: A program (malicious code) which, when executed, copies itself onto other media or files available to the computer executing it.

Virus screening software: Commercially available software that searches for certain bit patterns or other evidence of computer virus infection.

Appendix C: Department of Administration Security Council Members

Division	Member	Telephone	Email
DISC-BOT	Andy Scharf	296-3463	andy.scharf@state.ks.us
DISC-BAS	Bruce Roberts	296-3343	bruce.roberts@state.ks.us
DISC-BIS	Joe Hennes	296-3463	joe.hennes@state.ks.us
DISC-BOCS	Jerry Merryman	296-0999	jerry.merryman@state.ks.us
DISC-BOCS	John Voss	296-0999	john.voss@state.ks.us
DISC-BOT	Dave Timpany	296-6150	dave.timpany@state.ks.us
DISC-BDAS	Bill Cavalieri	296-5179	bill.cavalieri@state.ks.us
DISC	Duncan Friend	296-3463	duncan.friend@state.ks.us
DISC-BOT	Jim Logan	296-3343	jim.logan@state.ks.us
A & R	Daryl Daniels	296-2930	daryl.daniels@state.ks.us
DPS	Jan Cavalieri	296-4743	jan.cavalierie@state.ks.us
D of Budget	Jeff Arpin	296-2436	jeff.arpin@state.ks.us
D of Facilities	Kerry Ranabargar	296-1318	kerry.ranabargar@state.ks.us
Arch Svcs	Lee Ryan	296-8899	ryanl@doas.state.ks.us
DofA Legal	Mark Braun	296-6000	mark.braun@state.ks.us
Div of Printing	Verla Vines	296-2794	verla@ser06.ksleg.state.ks.us